UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,163	03/25/2004	Joshua T. Goodman	MS305314.1/MSFTP596US	6827

27195 7590 04/03/2008
AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	**PAPER NUMBER**
2136	
NOTIFICATION DATE	**DELIVERY MODE**
04/03/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
osteuball@thepatentattorneys.com

Office Action Summary	**Application No.** 10/809,163	**Applicant(s)** GOODMAN ET AL.
	Examiner FATOUMATA TRAORE	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16 and 18-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16 and 18-51* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *9/28/2007, 11/16/2007, 11/29/2007, 1/10/2008, 3/07/2008*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on December 28th, 2007.Claims 1, 6, 8,13,14, 18-20, 23, 31, 45, 46, 50 and 51have bee amended; Claim 17 has been cancelled. Claims 1-16 and 18-51 are pending and have been considered below.

Specification

2. The examiner acknowledges the amendment made to specification.

Claim Objections

3. The objection to claims 1, 17 and 46 has been withdrawn. However, the examiner is maintained the objection to claims 1-7, 9, 10, 12, 18-21, 28, 32, 33-38, 40, 45, 48, 49-51.

Claims 1-7, 9, 10, 12, 18-21, 28, 31, 33-38, 40, 45, 48, 49-51 are objected to because of the following informalities: the examiner notes the use of acronyms (e.g. URL, IP, SVM, etc.) throughout the claims without first including a description in plain text, as required. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The rejection is withdrawn in view of the amendment to claims 18, 19, 23 and 51.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Applicant is silent with respect to the rejection of claims 1-30 under 101. In any event, the amendment to claim 1 does not overcome the 101 rejection. Claim 1 recites a system. However, such system is made up of series of components, which are software per se. See page 6 of specification. In fact, claim 46 recites a computer readable medium having stored thereon the component of claim 1, which suggests that the “components” are software.

In respect to claims 23 and 45, the amendments do not overcome the 101 rejection. Claim 45 is still directed to a “data packet” not embodying on a computer readable medium see MPEP2106

As to claim23, there is no practical application. According, the rejections under 101 are sustained.

Double Patenting

6. The examiner acknowledges the filing of the terminal disclaimer. However, the double patenting rejection is maintained upton the acceptance of the terminal disclaimer.

Response to Arguments

7. Applicant's arguments filed December 28th, 2007 have been fully considered but they are not persuasive.

8. Applicant argues that " At page 14 of Office Action, Examiner erroneously asserts that Bandini et al. teaches, a third component that determines whether at least one IP address in the message is" any one of external or internal to the recipient's system via a machine learning technique with respect to dependent claim 17" however, the examiner respectfully disagrees and submits that Bandini et al discloses such feature see paragraphs [0011], [0026] *(The evaluation steps are made by reference to various attributes of an incoming message, including sender address, recipient list, subject, body, embedded URLs, and IP of sending relay. As may be appreciated, an evaluation on the basis of other attributes of the incoming message can alternatively be made as part of the e-mail filtering of the invention without departing from the teachings of the invention)*

9. *Applicant argued on page 15 of the reply that "nowhere teaches or suggests determining a true source of a message by way of tracing back through a received from list until an IP address is found that corresponds" to a fully qualified domain which corresponds" to an entry in the domain's MXrecord. Through this feature, the claimed invention facilitates determining true source of a message as a spammer may add as many URLs as he wants to the message" the examiner respectfully disagree and submits that Bandini et al discloses such feature see (paragraphs [0026], [0027], [0031], [00032]*.

10. There is no new ground of rejection when the basic thrust of the rejection remains the same. See In re Kronig, 539 F.2d 1300, 1302-03, 190 USPQ 425, 426-27 (CCPA 1976) To the extent that the response to the applicant's arguments may have mentioned new portions of the prior art references, which were not used in the prior office action, this does not constitute new a new ground of rejection. It is clear that the

prior art reference is of record and has been considered entirely by applicant. See In re Boyer, 363 F.2d 455,458 n.2, 150 USPQ 441,444, n.2 (CCPA 1966) and In re Bush, 296 F.2d 491,496, 131 USPQ 263,267 (CCPA 1961).

The mere fact that additional portions of the same reference may have been mentioned or relied upon does not constitute new ground of rejection. In re Meinhardt, 392, F.2d 273,280, 157 USPQ 270, 275 (CCPA 1968). Accordingly, this office action is being made final.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12. Claims 1-6, 8-14, 18-22, 31-34, 36-51 are rejected under 35 U.S.C. 102(e) as being anticipated by **Bandini et al** (US 2002/0199095).

Claim 1: **Bandini et al** discloses a system for filtering communication comprising:

a. A feature extraction component that receives an item and extracts a set of features associated (attribute data) with an origination of a message (sender address, subject, body, embedded URLs, and IP of sending relay) or part thereof and/or information that enables an intended recipient to contact or respond to the message (The e-mail relay 46 operates to intercept e-mail messages and extract attribute data from messages (step 52). The extracted attribute data is used to generate a comparison between the intercepted e-mail and e-mail message data in the SPAM database 37 (step 54)) (paragraphs [0020], [0026]); and

b. A feature analysis component that analyzes a subset of the extracted features in connection with building and employing a plurality of feature-specific filters that are independently trained to mitigate undue influence of at least one feature type over another in the message, the subset of extracted features comprising of at least one of a URL and an IP address, and the plurality of filters comprising at least a first feature-specific filter (Uniform Resource Locator (URL) included in an incoming message is compared to URLs contained records of the SPAM database 37 and Finally, in a related determination, the identity of the Internet Protocol (IP) address or Internet domain from which a SPAM message was received is compared to the IP address or Internet domains for the incoming message) (Paragraphs [0029]-[0032], Fig.2, Fig. 3); and

c. a machine learning component that determines whether at least one IP address in the message is any one of external or internal to the recipient's system via a machine learning technique(paragraphs [0011], [0026]).

Claim 2: **Bandini et al** discloses a system for filtering communication as in claim 1 above, and further discloses that a plurality of training components that individually employ at least one of IP addresses or URLs and other features, respectively, in connection with building the plurality of feature- specific filters)(Paragraphs [0029]-[0032], Fig.2, Fig. 3).

Claim 3: **Bandini et al** discloses a system for filtering communication as in claim 1 above, and further discloses that the first feature-specific filter is trained using IP addresses (the identity of the Internet Protocol (IP) address or Internet domain from which a SPAM message was received is compared to the IP address or Internet domains for the incoming message) (Paragraph [0032]).

Claim 4: **Bandini et al** discloses a system for filtering communication as in claim 1 above, and further discloses that the first feature-specific filter is trained using URLs ((Uniform Resource Locator (URL) included in an incoming message is compared to URLs contained records of the SPAM database 37) (Paragraph [0031]).

Claim 5: **Bandini et al** discloses a system for filtering communication as in claim 1 above, and further discloses that the plurality of feature specific filters comprising a second feature-specific filter that is trained using a subset of features extracted from the message other than a URL and an IP address (the subject filed of an incoming e-mail is compared to the subject field of records in the SPAM database 37 or In yet another evaluation, the body of the incoming message is compared to the body of messages in the SPAM database

37)(paragraphs [0029], [0030]).

Claims 6, 20: **Bandini et al** discloses a system for filtering communication comprising:

a. A feature extracting component that receives an item and extracts a set of features associated with an origination of a message or part thereof and/or information that enables an intended recipient to contact or respond to the message (The e-mail relay 46 operates to intercept e-mail messages and extract attribute data from messages (step 52). The extracted attribute data is used to generate a comparison between the intercepted e-mail and e-mail message data in the SPAM database 37 (step 54)) (paragraphs [0020], [0026]);

b. At least one filter that is used when one of the IP address of the message or at least some part of at least one of the URLs in the message is unknown/known (Uniform Resource Locator (URL) included in an incoming message is compared to URLs contained records of the SPAM database 37 and Finally, in a related determination, the identity of the Internet Protocol (IP) address or Internet domain from which a SPAM message was received is compared to the IP address or Internet domains for the incoming message) (Paragraphs [0029]-[0032], Fig.2, Fig. 3); and

c. a machine learning component that determines whether at least one IP address in the message is any one of external or internal to the recipient's system via a machine learning technique(paragraphs [0011], [0026]).

Claim 8: **Bandini et al** discloses a system for filtering communication as in claim 1 above, and further discloses that a filter combining component that combines information collected from the first and second feature-specific filters (the overall comparison match score, or level, is set by reference to a combination of one or more of the above discussed evaluations. In one embodiment, the overall SPAM likelihood is determined by assigning a weight to each evaluation and combining all weighed scores to arrive at the overall score)(paragraphs [0033], [0034], and Fig. 4).

Claims 9, 21: **Bandini et al** discloses a system for filtering communication as in claims 8 and 20 above, and further discloses that the first feature-specific filter detects at least one of known IP addresses and at least one known URL in the message (paragraphs [0031], [0032]).

Claims 10, 22: **Bandini et al** discloses a system for filtering communication as in claims 8 and 20 above, and further discloses that the second feature-specific filter detects non-IP address and non-URL data in the message (paragraphs [0028]-[0030]).

Claim 11: **Bandini et al** discloses a system for filtering communication as in claim 8 above, and further discloses that the filter combining component combines the information by at least one of multiplying scores generated by the filters, adding scores generated by the filters, or training an additional filter to combine the scores (add evaluation result to running comparison score according to relative weight) (paragraph [0023], Fig. 3 step 68).

Claim 13: **Bandini et al** discloses a system for filtering communication as in claim 6 above, and further discloses that the filter selection component that selects and employs at least one feature-specific filter out of the plurality of filters for which there is sufficient data extracted from the message (Fig. 3).

Claim 14: **Bandini et al** discloses a system for filtering communication as in claim 1 above, and further discloses that the first feature-specific filter is trained independently of a second feature-specific filter to mitigate either filter influencing the other when filtering the message (fig. 3 step 64 and step 80).

Claim 18: **Bandini et al** disclose the machine learning method as in claim 17 above, and further disclose that:

a. The component employs MX records to determine a true source of a message by way of tracing back through a received from list until an IP address is found that corresponds to a fully qualified domain which corresponds to an entry in the domain's MX record (in a related determination, the identity of the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message. The IP address or Internet domain of the sending relay is generally not enough on its own to indicate that a message is likely SPAM. However, a match of IP address or internet domain would enhance a finding of likely SPAM by reference to other evaluations)(paragraph [0032); and

b. Determines whether the IP address is external or internal by performing at least one of the following:

concluding that the IP address is in a form characteristic to internal IP addresses (paragraph [0032]); and

c. Performing at least one of an IP address lookup and a reverse IP address lookup to ascertain whether the IP address correlates with a sender's domain name (paragraph [0036]).

Claim 19: **Bandini et al** discloses the machine learning method as in claim 17 above, and further discloses that the component determines whether the IP address is external or internal comprises at least one of the following:

a. Collecting user feedback related to user classification of messages as spam or good (paragraph [0036], Fig. 3);

b. Examining messages classified as good by a user to learn which servers are internal (Fig. 3, step 72, 78); and

c. Finding a worst scoring IP address in a message (Fig. 3 step 70).

Claim 31: **Bandini et al** discloses a system for filtering communication comprising:

a. Providing a plurality of training data (The evaluation steps are made by reference to various attributes of an incoming message, including sender address, recipient list, subject, body, embedded URLs, and IP of sending relay. As may be appreciated, an evaluation on the basis of other attributes of the incoming message can alternatively be made as part of the e-mail filtering of the invention without departing from the teachings of the invention) (paragraph [0026]);

b. Extracting a plurality of feature types from the training data (Fig. 3 steps 64 and 80), the feature types comprising at least one IP address, at least one URL and text-based features (paragraphs [0031], [0032]); and

c. Training a plurality of feature-specific filters for the respective feature in an independent manner so that a first feature does not unduly influence a message score over a second feature type when determining whether a message is spam (paragraphs [0028]-[0032], Fig. 3).

d. Determining whether at least one IP address in the training data is any of external or internal to a recipient's system (paragraphs [0011], [0026]).

Claim 32: **Bandini et al** discloses a system for filtering communication as in claim 31 above, and further discloses that the plurality of training data comprises messages (paragraphs [0021], [0026], [0030]).

Claim 33: **Bandini et al** discloses a system for filtering communication as in claim 31 above, and further discloses that the plurality of feature-specific filters comprises at least two of the following:

a. A known IP address filter (paragraph [0032]);

b. An unknown IP address filter (paragraph [0032]);

c. A known URL filter (paragraph [0031]); an

d. Unknown URL filter (paragraph [0031]); and

e. A text-based filter (paragraph [0029], [0030]).

Claims 12, 36: **Bandini et al** discloses a system for filtering communication as in claims 6 and 33 above, and further discloses that the unknown IP address filter is trained using other messages comprising unknown IP addresses (paragraph [0032], Fig. 3).

Claim 34: **Bandini et al** discloses a system for filtering communication as in claim 33 above, and further discloses that the known IP address filter is trained using 32 bits of IP addresses (paragraph [0032], Fig. 3).

Claim 37: **Bandini et al** discloses a system for filtering communication as in claim 33 above, and further discloses that the text-based filter is trained using words, phrases, character runs, character strings, and any other relevant non-IP address or non-URL data in the message (paragraphs [0029], [0029]).

Claim 38: **Bandini et al** discloses a system for filtering communication as in claim 33 above, and further discloses a step of employing at least one of the known IP address filter, the unknown IP address filter, the known URL filter, and the unknown URL filter together with the text-based filter to more accurately determine whether a new message is spam (paragraphs [0029]-[0032], Fig. 3, Fig.4).

Claim 39: **Bandini et al** discloses a system for filtering communication as in claim 33 above, and further discloses a step of employing at least one of the feature-specific filters in connection with determining whether a new message is spam, such that the feature-specific filter is selected based in part on most relevant feature data observed in the new message (paragraphs [0029]-[0032], Fig. 3, Fig.4).

Claim 40: **Bandini et al** discloses a system for filtering communication as in claim 33 above, and further discloses that the URL filter is trained on URL data comprising a fully qualified domain name and subdomains of the fully qualified domain name (paragraph [0031], Fig. 3).

Claim 41: **Bandini et al** discloses a system for filtering communication as in claim 31 above, and further discloses a step of combining message scores generated from at least two filters used to scan a new message to generate a total score that facilitates determining whether the message is spam (paragraph [0023], Fig. 3 step 68).

Claim 42: **Bandini et al** discloses a system for filtering communication as in claim 41 above, and further discloses a step of combining message scores comprises at least one of the following: multiplying the scores; adding the scores; and training a new model to combine the scores (paragraph [0023], Fig. 3 step 68).

Claim 43: **Bandini et al** discloses a system for filtering communication as in claim 33 above, and further discloses that the combined with a feedback loop mechanism whereby users provide their feedback regarding incoming messages by submitting message classifications to fine tune the one or more feature-specific filters (paragraphs [0034]-[0036]).

Claim 44: **Bandini et al** discloses a system for filtering communication as in claim 31 above, and further discloses a step of quarantining messages that satisfy at least one criterion for a period of time until additional information about the message can be collected to update one or more feature-specific filters to facilitate determining whether the messages are spam (The attributes are employed to determine whether an e-mail message should be allowed to flow to the e-mail server 40 or should be diverted and subject to other action. Some of those actions, which the e-mail relay 46 is adapted to execute, include: quarantine the e-mail in the local message store database 38, reject the e-mail, and generate a special message to the intended recipient indicating that the e-mail message has been diverted)(paragraphs [0019], [0021], Fig. 2).

Claim 45: **Bandini et al** discloses a data packet adapted to be transmitted between two or more computer processes running on a machine-implemented system facilitating improved detection of spam (fig. 2), the data packet comprising: information associated with training a plurality of feature-specific filters in an independent manner to mitigate undue influence between features and employing at least one feature specific filter comprising an IP address filter or a URL filter to determine whether a message is spam and to determine whether at least on IP address in the message is any one of external or internal to a recipient's system(paragraphs [0011], [0026],[0028], [0040]).

Claim 46: **Bandini et al** discloses a system for filtering communication as in claim 1 above, and further discloses a computer readable medium having stored thereon the component of claim 1(paragraph [0013]).

Claim 47: **Bandini et al** discloses a system for filtering communication comprising a plurality of filters comprising at least one filter that is trained by using different smoothing for different spam features (paragraphs [0029]-[0032], Fig. 3 steps 64 and 80).

Claim 48: **Bandini et al** discloses a system for filtering communication as in claim 47 above, and further discloses that the feature is one of the following: an IP address or a portion thereof or a URL or a portion thereof (paragraphs [0029], [0030]).

Claim 49: **Bandini et al** discloses a system for filtering communication as in claim 48 above, and further discloses that at least one filter is trained by using different smoothing for different portions of at least one of an IP address or a URL (paragraphs [0031], [0032]).

Claim 50: **Bandini et al** discloses a system for filtering communication comprising:

a. Extracting data from a plurality of messages (paragraph [0026]);

b. Training at least one machine learning filter using at least a subset of the data, the training comprising employing a first smoothing for at least one of IP address or URL features and at least a second smoothing for other non-IP address or non-URL features (paragraphs [0031], [0032]).

c. Determine whether at least on IP address in the message is any one of external or internal to a recipient's system (paragraphs [0011], [0026]).

Claim 51: **Bandini et al** discloses a system for filtering communication as in claim 50 above, and further discloses that the smoothing (evaluation) differs in at least one of the following aspects:

a. The first smoothing comprises a different variance compared to the second smoothing with respect to a maximum entropy model (Fig. 3, step 64 and 80); and

b. The first smoothing comprises a different value of weight decay compared to the second smoothing with respect to an SVM model (paragraphs [0028]-[0032]).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 15, 16, 23-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bandini et al** (US 2002/0199095) in view of **Rothwell et al** (US 20030088627).

Claim 15: **Bandini et al** discloses a system for filtering communication as in claim 14 above, but does not explicitly discloses that at least one of the feature-specific filters models dependencies. However, **Rothwell et al** discloses an intelligent spam detection system, which further discloses that at least one of the feature-specific filters models dependencies (paragraph [0025]). Therefore, it would have been obvious to one of ordinary skills in the art at the time the invention was made to **Bandini et al** to use a model dependencies. One would have been motivated to do so in order to control delivery of unsolicited electronic mail and to provide a system that can dynamically detect unwanted SPAM electronic mail messages **Rothwell et all** (paragraph [0008]).

Claim 16: **Bandini et al** discloses a system for filtering communication as in claim 1 above, but does not explicitly discloses that the plurality of feature-specific filters is machine learning filters. However, **Rothwell et al** discloses an intelligent spam detection system, which further discloses that the plurality of feature-specific filters is machine-learning filters (a neutral analysis engine is used to determine whether a message is SPAM or not) (paragraph [0031], Fig. 1, and Fig. 3). Therefore, it would have been obvious to one of ordinary skills in the art at the time the invention was made to **Bandini et al** to use a machine learning system. One would have been motivated to do so in order to control delivery of unsolicited electronic mail and to provide a system that can dynamically detect unwanted SPAM electronic mail messages **Rothwell et all** (paragraph [0008]).

Claim 23: **Bandini et al** discloses a method implemented on a machine that optimizes an objective function of the form OBJECTIVE (MAXSCORE (ml), MAXSCORE (m2), ..., MAXSCORE(mk), wl...wn) where MAXSCORE(mk) =

MAX(SCORE(IPk,1), SCORE(IPk,2), ..., SCORE(IPk,kl)) where mk = messages; IPk,i represents the presence of some property(s) of ink; and SCORE(IPk,i) = the sum of the weights of the features of IPk,i. And where the machine learning method optimizes the weighs associated with one feature at any given time and maximizes accuracy on a training data (paragraphs ([0021] [0023], [0039], Figure .3). But does not explicitly disclose that the method is a machine learning method. However, **Rothwell et al** discloses an intelligent spam detection system, which further discloses a machine learning method (a neutral analysis engine is used to determine whether a message is SPAM or not) (paragraph [0031], Fig. 1, and Fig. 3). Therefore, it would have been obvious to one of ordinary skills in the art at the time the invention was made to **Bandini et al** to use a machine learning system. One would have been motivated to do so in order to control delivery of unsolicited electronic mail and to provide a system that can dynamically detect unwanted SPAM electronic mail messages **Rothwell et all** (paragraph [0008]).

Claim 24: **Bandini et al** and **Rothwell et all** disclose a machine learning method as in claim 23 above, and **Bandini et al** further discloses that the objective function depends in part on whether the messages are properly categorized as any one of spam or good (Fig3. step steps 78,76, 78, and 82).

Claim 25: **Bandini et al** and **Rothwell et all** disclose a machine learning method as in claim 23 above, and **Bandini et al** further discloses that. The machine learning method comprises a step of learning the weights for each feature in turn (In one embodiment, SPAM database records include a field for a submission count, corresponding to each SPAM message. The submission count is preferably used as part of the comparison formula to add weight to certain evaluations. For example, when a subject match is for a SPAM record with a high submission count, the subject match result should have an increased weight since the message is very likely to be a repeat of the SPAM message) (paragraphs [0023], [0033], [0039], Fig. 3 step 68).

Claim 26: **Bandini et al** and **Rothwell et all** disclose a machine learning method as in claim 25 above, and **Bandini et al** further discloses that the step of learning the weight for a given feature comprises sorting training instances comprising a property, the property comprising a feature in order by the weight at which the score for that message varies with the weight for that feature (paragraphs [0023], [0033], [0039], Fig. 3 step 68)

Claim 27: **Bandini et al** and **Rothwell et all** disclose a machine learning method as in claim 26 above, and **Bandini et al** further discloses that the training instances comprise electronic messages (paragraphs [0021], [0026], [0030]).

Claim 28: **Bandini et al** and **Rothwell et all** disclose a machine learning method as in claim 23 above, and **Bandini et al** further discloses that the messages are training instances and the property and the properties comprise one or more IP addresses that the message originated from and any URLs in the message (paragraphs [0031], [0032]).

Claim 29: **Bandini et al** and **Rothwell et all** disclose a machine learning method as in claim 23 above, and **Bandini et al** further discloses that the step of learning is performed using an approximation MAX(a1, a2, ..., an) is approximately equal to SUM(a1x, a2x, ..., anX)(l/x)(paragraphs ([0021][0023],[0039], Figure .3).

Claim 30: **Bandini et al** and **Rothwell et all** disclose a machine learning method as in claim 29 above, and **Bandini et al** further discloses that the objective function depends in part on whether the messages are properly categorized as spam or good (fig. 3 steps 72, 76, 78, 82).

15. Claims 7 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bandini et al** (US 2002/0199095) in view of **Jungck** (US 7,003,555).

Claims 7, 35: **Bandini et al** discloses a system for filtering communication as in claims 6 and 33 above, but does not explicitly discloses that the at least one filter is trained using some number of bits less than 32 bits of an IP address. However, Jungck discloses a system for enhancing the infrastructure of a network, which further discloses that at least one filter is trained using some number of bits less than 32 bits of an IP address (This 32 –bit IP address has two parts: one part identifies the source or destination sub-network (with the network number) and the other part identifies the specific machine or host within the source or destination sub-network (with the host number). An organization can use some of the bits in the machine or host part of the address to identify a specific sub-network within the sub-network. Effectively, the IP address then contains three parts: the sub-network number, an additional sub-network number, and the machine number) (column 8, lines 53-65). Therefore, it would have been obvious to one of ordinary skills in the art at the time the invention was made to **<u>Bandini et al</u>** to use part of the IP address in the filtering process. One would have been motivated to do so in order to identify the source of the received message.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

16. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

FT

Friday, March 28, 2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136